Oklahoma State Department of Education

Data Privacy Program Plan

December 2022

Table Of Contents

1. Introduction 1

1.1. Purpose 1

1.2. Osde Data Privacy Sharepoint For Information 1

2. Overview Of OSDE Privacy Program 1

2.1. Mission Statement 1

2.2. Strategic Goals And Objectives For Privacy 2

2.3. Data Privacy And Security Data Governance Subcommittee 3

2.4. Policies And Procedures Data Governance Subcommittee 3

3. Privacy Workforce Management 4

3.1. Senior Agency Official For Privacy (SAOP) 4

3.2. Data Privacy Program Manager 4

3.3. Chief Technology Officer (CTO) 4

4. Budget 4

5. Fair Information Practice Principles (FIPPS) 4

6. Privacy Risk Management Framework 6

7. Privacy Control Requirements 6

7.1. Osde Control Allocation 6

7.2. Osde Privacy Threshold Analysis (PTA) 6

7.3. Osde Privacy Impact Assessment (PIA) 7

7.4. System Of Records Notice (SORN) 7

8. Privacy Policy 7

9. Requirements For Handling And Protecting Personally Identifiable Information (PII)8

9.1. Recognizing PII 8

9.2. Minimizing The Collection Of PII 8

9.3. Handling And Transmitting PII.. 9

10. Breach Incident Response And Management 9

11. Awareness And Training 10

11.1. New Employee Orientation Training.. 10

11.2. Role-Based Training.. 10

12. Conclusion.. 10

Appendix A – Budget Plan 11

Appendix B – Security And Privacy Controls... 14

Appendix C – Program Development Schedule 19

1. Introduction

1.1. Purpose

The purpose of the Oklahoma State Department of Education (OSDE) Data Privacy Program Plan is to provide an overview of OSDE's Data Privacy Program (DPP). This plan, which is consistent with the requirements in the Office of Data Governance (ODG), *Oklahoma State Department of Education Data Modernization Strategic Plan 2023-2025* includes:

- A description of the structure of the DPP;
- The strategic goals and objectives of the DPP;
- The role of the privacy officials and staff;
- The resources dedicated to the DPP;
- The program management controls in place to meet applicable privacy requirements and manage privacy risks; and
- Any other information deemed necessary by the OSDE's DPP.

1.2. OSDE Data Privacy SharePoint for Information

The SharePoint page contains information about privacy compliance, safeguard information, training and awareness programs, policies and guidance, and contact information. OSDE Data Privacy and Security website is currently public and will be updated to include more current and accurate information for the public.

2. Overview of OSDE Data Privacy Program

2.1. Mission Statement

OSDE is committed to safeguarding the privacy of education data. The mission of the OSDE DPP is to preserve and enhance privacy protections for all individuals who entrust their personal information to the OSDE by embedding and enforcing privacy protections throughout all of OSDE's daily operations. OSDE strives to be a leader in education privacy policy and best practices.

The DPP prioritizes and implements legal compliance with the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and Protection of Pupil Rights Amendment (PPRA) as well as policy directives and best practices issued in furtherance of the Act. The program adheres to the policy framework embodied in the Fair Information Practice Principle (FIPPs) to ensure that individual privacy is protected throughout the collection, retention, maintenance, use, dissemination, disclosure, and disposal of all personally identifiable information (PII) maintained by the OSDE.

OSDE's DPP is co-led by OSDE's Office of Data Governance (ODG) and Office of Management and Enterprise Services (OMES). The DPP carries out the following core functions:

- Develops and administers OSDE's privacy policies, guidelines and procedures;

- Provide performance metrics and reports as required, or as needed to reduce privacy risks;
- Monitor for privacy changes to State and/or Federal laws, regulations, and policies;
- Assesses all new or proposed programs, systems, technologies, and processes for privacy risks and provides recommendations to strengthen privacy protections;
- Provides privacy awareness training and targeted privacy trainings to OSDE personnel;
- Provide privacy guidance and best practices to the Districts;
- Ensure privacy policies are posted on OSDE websites and/or other digital services where appropriate;
- Collaborates with OMES Office of Cyber Command to implement and operationalize policies and tools to secure the confidentiality, integrity, and availability of OSDE's information and information systems;
- Operates a data breach response program to ensure that all incidents involving personally identifiable information (PII) are properly reported, investigated, and mitigated, as appropriate; and
- Maintains updated privacy artifacts in compliance with legal requirements (e.g., FERPA, PPRA).

2.2. Strategic Goals and Objectives for Privacy

OSDE's DPP supports all six priorities in the Oklahoma State Department of Education Data Modernization Strategic Plan 2023-2025 to accelerate and mature security and privacy functions across the OSDE and Districts, as well as the important goal to build privacy and security that works for everyone. To accomplish the strategic outcomes, three OSDE long-term goals are created, each supported by specific and measurable objectives.

Goal 1 – Advance the maturity of OSDE's privacy policies, procedures, and best practices.

- Objective 1.1 – Maintain compliance with privacy laws, regulations, and best practices by enhancing and regularly updating OSDE's privacy documents.
- Objective 1.2 – Provide guidance to OSDE's offices concerning the implementation of with privacy laws, regulations, and best practices, supported by the legal advice from the OSDE Legal Service department.
- Objective 1.3 – Ensure that privacy-related complaints and incidents at OSDE are reported systematically, efficiently processed, and appropriately mitigated in accordance with legal requirements and OSDE policies and procedures.

Goal 2 – Proactively and pragmatically manage privacy risk.

- Objective 2.1 – Provide guidance and issue policies related to privacy by leveraging the expertise of Office of Data Governance members and Privacy and

Security experts from OMES. Build effective communication channels between OSDE and OMES Cyber Command Office.

- Objective 2.2 – Leverage the expertise of oversight and advisory bodies, advocates, and privacy experts from the private sector to foster dialogue and learn about emerging issues.
- Objective 2.3 – Understand the PII collected from each office by collecting information from the Data Dictionary. Create and maintain annual PII inventory.
- Objective 2.4 – Establish Metrics to track the effectiveness of the OSDE's DPP.

Goal 3 – Foster a culture of privacy and demonstrate state leadership through policy and partnerships.

- Objective 3.1 – Partner with the OSDE Chief Technology Officer (CTO) on key initiatives that promote privacy, including embedding privacy in the development lifecycle.
- Objective 3.2 – Develop and deliver targeted, role-based training for employees with specialized roles and other key stakeholders across OSDE.
- Objective 3.3 – Provide advice and guidance to OSDE offices on complicated privacy issues.

2.3. Data Privacy and Security Data Governance Subcommittee

Data Privacy and Security Data Governance Subcommittee, established by OSDE Data Governance Board, works to establish and ensure compliance with data privacy and security standards and best practices. The core functions of the Data Privacy and Security Subcommittee include creating policies and documentation that promote best practices around data privacy and security and advocating for and supporting effective staff training on data privacy and security. The Data Privacy and Security Subcommittee members include the Data Privacy Program Manager, Executive Director of Data Governance, Executive Director of Data & Information Systems, and Open Records Coordinator.

The Data Privacy and Security Subcommittee convenes weekly and routinely reviews OSDE privacy policies and processes and identifies opportunities for strengthening, clarifying, and improving them, as well as identifies and recommends privacy training opportunities for OSDE employees, as appropriate.

2.4. Policies and Procedures Data Governance Subcommittee

Policies and Procedures Data Governance Subcommittee, established by OSDE Data Governance Board (DGB), works to review, update, and disseminate data governance policies and procedures. The core functions of Policies and Procedures Subcommittee include compiling and maintaining a master list of DG related policies & procedures, ensuring data governance policies and procedures are widely known and consistently applied, and advocating for staff training on data governance. The Policies and Procedures Subcommittee members include Executive Director of Data Governance, Executive Director of Accountability, Director of Data Project Management, Federal Programs Director of Compliance & Monitoring, and Data Privacy Program Manager.

The Policies and Procedures Subcommittee convenes bi-weekly and routinely reviews OSDE data governance policies and identifies opportunities for strengthening, clarifying, and improving them.

3. Privacy Workforce Management

3.1. Senior Agency Official for Privacy (SAOP)

The Office of Data Governance provides oversight and management of OSDE's DPP. The Executive Director of Data Governance serves as OSDE's Senior Agency Official for Privacy (SAOP). The SAOP assesses and addresses the hiring, training, and professional development needs of OSDE with respect to privacy, including providing input into the performance of the Data Privacy Program Manager. Additionally, the SAOP coordinates with the Chief Technology Officer to maintain and enhance a current workforce planning process.

3.2. Data Privacy Program Manager

The Data Privacy Program Manager manages OSDE privacy and related compliance activities, reviews applicable OSDE privacy artifacts, includes but not limited to system of records notices (SORNs), PIAs, privacy threshold analysis (PTAs) and data sharing agreements, and Oversees training, reporting, and consultation requirements. The Data Privacy Program Manager ensures the SAOP is notified of all breaches of PII within ONE HOUR of receiving notification and develops competency requirements for OSDE staff in the area of PII breach response.

3.3. Chief Technology Officer (CTO)

The OSDE CTO Advises and provides cyber security and information technology subject matter expertise to the SAOP and the Privacy Program Manager to identify ways in which the OSDE can safeguard privacy information. CTO also Provides current threat information regarding the compromise of PII and information systems containing PII.

4. Budget

The SAOP ensures that OSDE identifies and plans for the resources needed to implement the DPP each year. The SAOP collaborates with Financial Services, Comptroller & Oklahoma Cost Accounting System (OCAS) Leadership, to review investment plans and budgetary requests to ensure that privacy requirements and associated privacy controls are identified and collaborates with key stakeholders to ensure privacy risks are addressed to the maximum extent possible. The annual operational costs in Appendix A are expected for fiscal year 2022-23.

5. Fair Information Practice Principles (FIPPs)

The OSDE DPP adheres to the FIPPs. The FIPPs are a collection of widely accepted principles that both federal and state agencies use when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs includes:

- Access and Amendment.

OSDE regularly collects, stores, and shares personally identifiable data from public schools and school districts for a variety of purposes, including but not limited to compliance with federal and state laws and regulations. Individuals are provided with appropriate access to their PII collected by OSDE and the opportunity to correct or amend the PII.

- Accountability.

OSDE monitor, audit, and document compliance. OSDE is accountable for complying with FIPPs and applicable privacy requirements. OSDE creates and maintain user access level directory to define the roles and responsibilities with respect to PII for all employees and contractors. OSDE also provide appropriate training to all employees and contractors who have access to PII.

- Authority.

OSDE limits the PII which it creates, collects, uses, processes, stores, maintains, disseminates, and discloses to what is directly relevant and necessary to accomplish the legally authorized purpose. OSDE identifies the authority in the appropriate notices.

- Minimization.

OSDE limits the PII which it creates, collects, uses, processes, stores, maintains, disseminates, or discloses to what is directly relevant and necessary to accomplish a legally authorized purpose, and only maintain PII for as long as is necessary to accomplish the purpose.

- Quality and Integrity.

OSDE creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII with the accuracy, relevance, timeliness, and completeness, as is reasonably necessary, to ensure fairness to the individual.

- Individual Participation.

Individuals are involved in the process of using PII and, to the extent practicable, individual consent is granted for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Individuals may address concerns or complaints to SAOP.

- Purpose Specification and Use Limitation.

OSDE provides notice of the specific purpose for which PII is collected and only uses, processes, stores, maintains, disseminates, and discloses PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

- Security.

OSDE ensures that administrative, technical, and physical safeguards are established to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

- Transparency.

OSDE provides clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

6. Privacy Risk Management Framework

OSDE adhere to the process described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organization*, SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, and *The NIST Privacy Framework*. OSDE collaborates with OMES to embrace privacy and security through daily operations.

7. Privacy Control Requirements

OSDE has implemented NIST SP 800-53, Rev. 5 Chapter C to ensure compliance with applicable statutory, regulatory, and policy requirements with respect to information privacy and security. OSDE Privacy Program Manager is in the process of establishing privacy controls in compliance with NIST SP 800-53, Rev. 5 Chapter C. The privacy control tools are used to measure the privacy compliance process cycle. Four key parts of the privacy compliance process cycle includes: Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), System of Records Notice (SORN), and privacy review.

7.1. OSDE Control Allocation

OSDE controls are designed to facilitate risk management and compliance with applicable federal and state laws, executive orders, directives, regulations, policies, and standards. These controls are expected to change over time as controls are withdrawn, revised, and added. Proposed modifications to the controls are carefully analyzed during each revision cycle. The objective is to adjust the level of information security and privacy over time to meet the needs of OSDE. *See* Appendix B.

7.2. OSDE Privacy Threshold Analysis (PTA)

A privacy threshold analysis is a questionnaire used to determine if a system contains personally identifiable information (PII), whether a PIA is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. A PTA should be completed when proposing a new information technology system through the budget process that will collect, store, or process identifiable information or when starting to develop or significantly modify such a system, or when a new electronic collection of identifiable information is being proposed. The OSDE privacy manager reviews the PTA to determine if the system or program is privacy-sensitive and requires additional privacy compliance documentation such as a PIA or SORN. PTAs expire and must be reviewed and re-certified every year or when changes/updates occur.

7.3. OSDE Privacy Impact Assessment (PIA)

The PIA is a decision tool used by OSDE and OMES to identify and mitigate privacy risks of systems and programs (1) what PII OSDE is collecting; (2) why the PII is being collected; and (3) how the PII will be collected, used, accessed, shared, safeguarded, and stored. PIAs assess risk by applying the universally recognized Fair Information Practice Principles to OSDE systems and programs. If a PIA is required, the program manager will work with the OMES to write the PIA for submission to the Office of Data Governance Security and Privacy Subcommittee for review and approval by the Chief Information Officer.

7.4. System of Records Notice (SORN)

The 62 O.S. 34.11.10, the Oklahoma State Government Security Breach Transparency Initiative requires that the Oklahoma Chief Information Officer shall develop and maintain an online web presence for the public to access information on certain security breaches. The Office of Data Governance keeps SORN records to better monitor and react to any data breaches related to OSDE. A SORN is utilized to provide the notice regarding PII collected in a system of records. SORNs explain how the information is used, retained, and may be accessed or corrected, and whether certain portions of the system are subject to FERPA or HIPPA exemptions for law enforcement, national security, or other reasons. If a SORN is required, the program manager will work with the Data Privacy Program Manager and OMES to write the SORN for submission to the Office of Data Governance for review and approval by the Chief Information Officer.

8. Privacy Policy

OSDE has developed a privacy policy that establishes a set of privacy principles and applies those principles to employees, individuals applying for OSDE programs, research partners, contractors and school districts. These principles and policy requirements govern how OSDE identifies, processes, and minimizes PII and explains how OSDE complies with the privacy requirements.

OSDE will be accountable for complying with these principles, providing training to personnel who use or process PII, and auditing the actual use of PII to demonstrate compliance with these principles and applicable privacy protection requirements.

- Information Access and Security
    - Data Privacy Policy
    - Data Security Policy
    - Data Sharing Agreement Policy

    - Information Security Incident Reporting Policy
    - Personal Identifier Information Policy
        - Student Data Policy
        - Teacher Social Security Number Policy
    - User Account Policy
    - Data Retention and Destruction Policy
- Systems and Network Security
    - Acceptable System Use Policy
    - Acceptable Network Use Policy
    - Acceptable Email Use Policy
- Family Educational Rights and Privacy Act (FERPA) Policy
- Vendor Policy

9. Requirements for Handling and Protecting Personally Identifiable Information (PII)

9.1. Recognizing PII

Personally identifiable information for education records is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. According to 34 CFR § 99.3 , PII includes, but is not limited to:

1) The student's name;
2) The name of the student's parent or other family members;
3) The address of the student or student's family;
4) A personal identifier, such as the student's social security number, student number, or biometric record;
5) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
7) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

9.2. Minimizing the Collection of PII

OSDE maintains an inventory of PII holdings and uses the PAS, PIA, and SORN certification and re-certification process to identify reduction opportunities and to ensure, to the maximum extent practicable, that such holding is accurate, relevant, timely, and complete. In addition, OSDE has established process requirements for justifying the collection, maintenance, and uses of SSNs as directed in the OSDE Privacy and Security Policies.

9.3. Handling and Transmitting PII

PII requires strict handling guidelines due to the nature of the PII and the increased risk to an individual if data were to be compromised. OSDE provides guidelines and procedures for employees and contractors who handle PII. Methods for handling PII include, but are not limited to:

Store and encrypt sensitive PII on secure OSDE networks, computers, media, and other devices;

- Lock or log off unattended computer systems;
- Secure sensitive paper PII data by locking it in desks and filing cabinets;
- Only use OSDE-provided e-mail addresses for conducting official business;
- Destroy sensitive paper PII by shredding; and
- Delete sensitive electronic PII by emptying computer recycle bin.

Sensitive PII may be distributed or released to other individuals only if: (1) it is within the scope of the recipient's official duties; (2) the recipient has an official, job-based need to know; (3) the distribution is done in accordance with a legitimate underlying authority (e.g., a routine use specified in a SORN); and (4) sharing information is done in a secure manner. When in doubt, all OSDE employees must treat PII as sensitive and must keep the transmission of sensitive PII to a minimum, even when transmission would occur by secure means.

10. Breach Incident Response and Management

A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.

All OSDE employees and contractors must immediately report any potential or actual incidents to OSDE's Incident Response Team (IRT) as soon as they become aware that an incident may have occurred using a Breach Incident Form. The form will automatically send a report to the IRT at the Office of Data Governance.

The SAOP and data privacy manager must determine which remediation methods should be used in the event of an actual compromise of PII based on the type of harm caused to the individual(s), based on the Breach Response Plan (BRP). The IRT must investigate the facts and circumstances surrounding the potential incident and, if PII may have been involved. The IRT also develops after action reports for high- and moderate-risk incidents, which document the details of the incidents and the steps taken to remediate the gaps which caused the incident to occur, and conducts an annual table-top exercise, which consists of a structured, readiness-testing activity, which simulates an actual incident involving PII designed to prepare key stakeholders and decision-makers for an emergency involving a data breach.

11. Awareness and Training

OSDE requires all employees and contractors to complete privacy training when first beginning work and annually thereafter. More mandatory in-depth cybersecurity and privacy trainings are planned and will be required in every employee's performance plan. OSDE also conduct activities and community outreaches promoting security awareness, such as Security Awareness Day.

11.1. New Employee Orientation Training

OSDE, working with OMES Cyber Command, conducts its new employee training through the Security Education Awareness Training (SEAT).

11.2. Role-Based Training

In addition to new-hire and annual privacy training requirements, OSDE provides role-based training to employees with specialized roles on a periodic basis, focusing on how employees in various OSDE Offices should leverage the policies and procedures and best practices as part of their official duties.

12. Conclusion

OSDE is committed to safeguarding PII that students, teachers, parents and employees entrust to the agency. Privacy considerations are embedded in all levels of decision-making and operations in an effort to continue to build a culture of trust and privacy at the OSDE. For Program Development Schedule, *see* Appendix C.

Appendix A – Budget Plan

Item	Project	Budget Estimate	Description
1	Data Inventory, Discovery, & Classification	14%	This specific work focuses on generating a data catalog, creating a data mapping project, implementing manual and automated identification and discovery of data, and leading a process for data sensitivity that provides a tagged and structured understanding of data at rest and in motion.
2	Privacy Program Management	22%	This work could include identifying and implementing privacy governance and management solutions, risk and compliance dashboards, risk response and a mitigation plan with procedures and possible utilities, and penetration testing to find security vulnerabilities in current systems to prevent future data leaks or security breaches.
3	Security and Privacy Internal Risk Management	22%	This specific work would focus on: - Internal systems ongoing evaluation and assessment processes, products, and services for regular and real-time risk reporting. This could include a purchase or build of a system along with required maintenance and operations, - Security and privacy plans of action project centered around rapidly defining actions and projects when new privacy or security needs arise - Continuity with the OMES 3rd party risk assessment program-extended process/procedure build-out for a privacy impact assessment, data protection impact assessment, and vendor

			screenings. In addition, an internal vendor audit process would be created to assure alignment with OMES over time. Continuity with OMES standards/policies- procedure and process examination and build out to ensure conformance and efficiency in execution against OMES standards.
4	Security and Privacy Consulting	15%	In addition to the consulting necessary for the above work, this would provide the experts to help lead and guide the overall work.
5	Training, Awareness, and Professional Learning	14%	This would center on training for internal OSDE staff, as well as districts, and could include: - Training content modules - Awareness campaigns - Professional learning events and opportunities - Additions to the Center of Excellence - Privacy program aids (inventory, classification, 3rdparty, public transparency, etc). In addition, supports for the common shared library of EdTech resource profiles, common contracts for reuse, etc. - Security program aids (response plans, phishing, scanning, pentest, vulnerability, etc).
6	Other Security Enhancing Technologies	14%	These technologies would help in strengthening security and could include technologies such as manual penetration testing and ethical hacking, automated vulnerability scanning, or a client device program (enhance availability and use of tools like secure messaging and file sharing, privacy filters, secure

			searching, external storage, personal devices, etc.)

Appendix B – Security and Privacy Controls

Control	Control Code	Control Name
Access Control	AC-1	Policy and Procedures
	AC-2	Account Management
	AC-3	Access Enforcement
	AC-5	Separation of Duties
	AC-6	Least Privilege
	AC-21	Information Sharing
	AC-22	Publicly Accessible Content
Awareness and Training	AT-1	Policy and Procedures
	AT-2	Literacy Training and Awareness
	AT-3	Role-Based Training
	AT-4	Training Records
	AT-6	Training Feedback
Audit and Accountability	AU-1	Policy and Procedures
	AU-2	Event Logging
	AU-3	Content of Audit Records
	AU-4	Audit Log Storage Capacity
	AU-5	Response to Audit Logging Process Failures
	AU-6	Audit Record Review, Analysis, and Reporting
	AU-7	Audit Record Reduction and Report Generation
	AU-8	Time Stamps
	AU-9	Protection of Audit Information
	AU-10	Non-repudiation
	AU-11	Audit Record Retention
	AU-12	Audit Record Generation
	AU-13	Monitoring for Information Disclosure
	AU-14	Session Audit
	AU-16	Cross-Organizational Audit Logging
Assessment, Authorization, and Monitoring	CA-1	Policy and Procedures
	CA-2	Control Assessments
	CA-3	Information Exchange
	CA-5	Plan of Action and Milestones
	CA-6	Authorization
	CA-7	Continuous Monitoring
	CA-9	Internal System Connections
Configuration Management	CM-1	Policy and Procedures
	CM-2	Baseline Configuration
	CM-3	Configuration Change Control
	CM-4	Impact Analyses
	CM-5	Access Restrictions for Change
	CM-6	Configuration Settings

	CM-7	Least Functionality
	CM-8	System Component Inventory
	CM-9	Configuration Management Plan
	CM-10	Software Usage Restrictions
	CM-11	User-Installed Software
	CM-12	Information Location
	CM-13	Data Action Mapping
	CM-14	Signed Components
Contingency Planning	CP-1	Policy and Procedures
	CP-2	Contingency Plan
	CP-3	Contingency Training
	CP-4	Contingency Plan Testing
	CP-6	Alternate Storage Site
	CP-7	Alternate Processing Site
	CP-8	Telecommunications Services
	CP-9	System Backup
	CP-10	System Recovery and Reconstitution
	CP-11	Alternate Communications Protocols
	CP-12	Safe Mode
	CP-13	Alternative Security Mechanisms
Identification and Authentication	IA-1	Policy and Procedures
	IA-2	Identification and Authentication (Organizational Users)
	IA-4	Identifier Management
	IA-5	Authenticator Management
	IA-6	Authentication Feedback
	IA-8	Identification and Authentication (Non-Organizational Users)
	IA-9	Service Identification and Authentication
	IA-11	Re-authentication
	IA-12	Identity Proofing
Incident Response	IR-1	Policy and Procedures
	IR-2	Incident Response Training
	IR-3	Incident Response Testing
	IR-4	Incident Handling
	IR-5	Incident Monitoring
	IR-6	Incident Reporting
	IR-7	Incident Response Assistance
	IR-8	Incident Response Plan
Maintenance	MA-1	Policy and Procedures
	MA-2	Controlled Maintenance
	MA-3	Maintenance Tools
	MA-4	Nonlocal Maintenance

Physical and Environmental Protection	PE-1	Policy and Procedures
	PE-2	Physical Access Authorizations
	PE-3	Physical Access Control
	PE-4	Access Control for Transmission
	PE-5	Access Control for Output Devices
	PE-8	Visitor Access Records
	PE-9	Power Equipment and Cabling
	PE-10	Emergency Shutoff
	PE-11	Emergency Power
	PE-12	Emergency Lighting
	PE-13	Fire Protection
	PE-14	Environmental Controls
	PE-15	Water Damage Protection
	PE-17	Alternate Work Site
	PE-21	Asset Monitoring and Tracking
Planning	PL-1	Policy and Procedures
	PL-2	System Security and Privacy Plans
	PL-4	Rules of Behavior
	PL-7	Concept of Operations
	PL-8	Security and Privacy Architectures
Program Management	PM-1	Information Security Program Plan
	PM-2	Information Security Program Leadership Role
	PM-3	Information Security and Privacy Resources
	PM-4	Plan of Action and Milestones Process
	PM-5	System Inventory
	PM-6	Measures of Performance
	PM-8	Critical Infrastructure Plan
	PM-9	Risk Management Strategy
	PM-10	Authorization Process
	PM-11	Mission and Business Process Definition
	PM-12	Insider Threat Program
	PM-13	Security and Privacy Workforce
	PM-14	Testing, Training, and Monitoring
	PM-15	Security and Privacy Groups and Associations
	PM-16	Threat Awareness Program
	PM-17	Protecting Controlled Unclassified Information on External Systems
	PM-18	Privacy Program Plan
	PM-19	Privacy Program Leadership Role
	PM-20	Dissemination of Privacy Program Information
	PM-21	Accounting of Disclosures
	PM-22	Personally Identifiable Information Quality Management
	PM-23	Data Governance Body

	PM-24	Data Integrity Board
	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research
	PM-26	Complaint Management
	PM-27	Privacy Reporting
	PM-28	Risk Framing
	PM-29	Risk Management Program Leadership Roles
	PM-31	Continuous Monitoring Strategy
Personnel Security	PS-1	Policy and Procedures
	PS-2	Position Risk Designation
	PS-3	Personnel Screening
	PS-4	Personnel Termination
	PS-5	Personnel Transfer
	PS-6	Access Agreements
	PS-7	External Personnel Security
	PS-9	Position Descriptions
Personal Identifiable Information Processing and Transparency	PT-1	Policy and Procedures
	PT-2	Authority to Process Personally Identifiable Information
	PT-3	Personally Identifiable Information Processing Purposes
	PT-4	Consent
	PT-5	Privacy Notice
	PT-6	System of Records Notice
	PT-7	Specific Categories of Personally Identifiable Information
	PT-8	Computer Matching Requirements
Risk Assessment	RA-1	Policy and Procedures
	RA-2	Security Categorization
	RA-3	Risk Assessment
	RA-5	Vulnerability Monitoring and Scanning
	RA-6	Technical Surveillance Countermeasures Survey
	RA-7	Risk Response
	RA-8	Privacy Impact Assessments
	RA-9	Criticality Analysis
	RA-10	Threat Hunting
System and Services Acquisition	SA-1	Policy and Procedures
	SA-2	Allocation of Resources
	SA-3	System Development Life Cycle
	SA-4	Acquisition Process
	SA-5	System Documentation
	SA-8	Security and Privacy Engineering Principles

	SA-9	External System Services
	SA-17	Developer Security and Privacy Architecture and Design
	SA-20	Customized Development of Critical Components
	SA-22	Unsupported System Components
System and Communications Protection	SC-1	Policy and Procedures
	SC-2	Separation of System and User Functionality
	SC-3	Security Function Isolation
	SC-4	Information in Shared System Resources
	SC-5	Denial-of-Service Protection
	SC-6	Resource Availability
	SC-7	Boundary Protection
	SC-8	Transmission Confidentiality and Integrity
	SC-15	Collaborative Computing Devices and Applications
	SC-16	Transmission of Security and Privacy Attributes
System and Information Integrity	SI-1	Policy and Procedures
	SI-4	System Monitoring
	SI-5	Security Alerts, Advisories, and Directives
	SI-6	Security and Privacy Function Verification
	SI-7	Software, Firmware, and Information Integrity
	SI-8	Spam Protection
	SI-10	Information Input Validation
	SI-11	Error Handling
	SI-12	Information Management and Retention
	SI-13	Predictable Failure Prevention
	SI-14	Non-Persistence
	SI-15	Information Output Filtering
	SI-17	Fail-Safe Procedures
	SI-18	Personally Identifiable Information Quality Operations
	SI-19	De-Identification

Appendix C – Program Development Schedule

	Milestones	**Person or Team Responsible**	**Planned Completion Time**
Policies, Procedures and Best Practices	Data Privacy Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Data Security Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Data Sharing Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Information Security Incident Reporting Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee; OMES Cyber Command Office	FY-2023
	Personal Identifier Information Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	User Account Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and	FY-2023

		Procedures Subcommittee	
	Data Retention and Destruction Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Acceptable System Use Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Acceptable Network Use Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Acceptable Email Use Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Family Educational Rights and Privacy Act (FERPA) Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Vendor Policy	Privacy Manager; Data Privacy and Security Subcommittee; Policies and Procedures Subcommittee	FY-2023
	Accountability Reporting		FY-2023

PIA, PTA and SORN Review and Certification	Accreditation/Highly Qualified Teacher/School Improvement	Privacy Manager; Data Privacy and Security Subcommittee	FY-2023
	Allocation Notices		FY-2023
	Alternative Education Implementation Plan		FY-2023
	Annual Incident and Firearms Report- Unsafe School Choice Option Report		FY-2023
	Aware		FY-2023
	Bus Driver Certification		FY-2023
	Child Nutrition - Child and Adult Care Food Program Claims App		FY-2023
	Child Nutrition - Child and Adult Care Food Program Inspect Service		FY-2023
	Child Nutrition - Child and Adult Care Food Program Main App		FY-2023
	Child Nutrition - National School Lunch Program Admin Review		FY-2023
	Child Nutrition - National School Lunch Program Claims App		FY-2023
	Child Nutrition - National School Lunch Program Main App		FY-2023
	Child Nutrition - Summer Food Program		FY-2023
	Child Nutrition – Eclaims		FY-2023
	Child Passport Webservices		FY-2023
	Class Size		FY-2023
	District & School Administration		FY-2023
	District Bullying Prevention Policy		FY-2023
	District Ownership Wizard		FY-2023
	Districtwide Student Needs Assessment		FY-2023
	Early Learning Dashboard		FY-2023
	EDPLan		FY-2023
	Education for Homeless Children and Youth District Census Report		FY-2023
	Gifted and Talented		FY-2023

	Grants Management and Expenditure Reporting		FY-2023
	Language Instruction for English Learners and Immigrant Students Annual Performance Report		FY-2023
	Migrant Information System 2000		FY-2023
	Non-Standard Accommodation		FY-2023
	Oklahoma Cost Accounting System (OCAS)		FY-2023
	Oklahoma Academic Scholars		FY-2023
	Oklahoma Annual District Technology Survey		FY-2023
	Oklahoma Educator Credentialing System		FY-2023
	Payment Notices		FY-2023
	Reading Sufficiency Act (RSA) Annual District Reading Plan		FY-2023
	Reading Sufficiency Act Survey		FY-2023
	School Board Tracking System		FY-2023
	School Personnel Records		FY-2023
	School Personnel Records - Secure Upload Application		FY-2023
	Seal of Biliteracy Report		FY-2023
	Single Sign On (SSO)		FY-2023
	Special Education - Child Count		FY-2023
	State Aid Flexible Benefit Allowance		FY-2023
	State Aid Management System (SAMS)		FY-2023
	State Infection Reporting System (SIRS)		FY-2023
	State Testing Number (STN) /xDUID		FY-2023
	State Vision Screening		FY-2023
	Student Transfer System		FY-2023
	Teacher Leader Effectiveness		FY-2023
	Title I Part D, Subpart 2 - Local Education Agency (LEA) Programs for Children/Youth who are Neglected, Delinquent or At-Risk		FY-2023

	Title I, Part A and Title V, Part B Report		FY-2023
	Title I, Part D, Subpart 1		FY-2023
	Transparency Website		FY-2023
	WAVE		FY-2023
Administrative Tasks	FY23 Annual Privacy Report	Privacy Manager	FY-2024
	Annual Review of Privacy websites for compliance	Privacy Manager	FY-2023
	Complete and SEAT training for all OSDE employees, contractors, etc.	Privacy Manager	FY-2023
	Develop and deploy at least five role-based training modules	Privacy Manager	FY-2023
	Employee awareness and outreach to agencies/offices	Privacy Manager	FY-2023